

AMENDMENTS TO THE CLAIMS

Please cancel claim 25, amend claim 1, 6, 19, 24, 39, and insert new claims 52-56, as follow. A complete listing of the claims is provided below.

1. (Currently Amended) A method for managing user access information for access to one or more database network nodes, the method comprising:
 - storing database user authorization in a central directory that is ~~connected~~ associated with to one or more ~~databases~~ network nodes, the database user authorization comprising a user role; ~~the user role comprising one or more privileges;~~
 - storing database user authentication information;
 - locally ~~defining~~ associating the user role that is at the central directory with one or more privileges, wherein the act of locally associating is performed at a one of the network node nodes that is associated with the central directory;
 - receiving an access request from a user for the network node;
 - authenticating the user based upon the database user authentication information; and
 - granting the user privileges on the network node based upon the user role;
 - wherein the database user authorization is stored as one or more data objects in the central directory, ~~and one of the one or more data objects comprises a distinguished name that does not include a user name.~~
2. (Original) The method of claim 1 in which the central directory comprises a LDAP-compatible directory.
3. (Original) The method of claim 1 in which the database user authentication information is stored at the central directory.
4. (Original) The method of claim 1 in which the database user authorization is stored in a schema having a hierarchy of schema objects.

5. (Original) The method of claim 4 in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.
6. (Currently Amended) The method of claim 5 in which the one or more privileges associated with the ~~one or more locally defined roles~~ are assigned to the one or more users.
7. (Original) The method of claim 4 in which the hierarchy of schema objects comprises a enterprise domain, wherein the enterprise domain comprises one or more enterprise roles.
8. (Original) The method of claim 7 in which each of the one or more enterprise roles is associated with one or more users and one or more locally defined roles.
9. (Original) The method of claim 7 in which the enterprise domain is associated with one or more network nodes.
10. (Canceled)
11. (Previously Presented) The method of claim 1 in which the one or more data objects are stored in a security subtree in the central directory.
12. (Original) The method of claim 1 in which administrative access is controlled to one or more data objects in the central directory.
13. (Original) The method of claim 12 in which access control is implemented using an access control point associated with the one or more data objects in the central directory.
14. (Original) The method of claim 13 in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory.

15. (Original) The method of claim 13 in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory.
16. (Original) The method of claim 13 in which the access control point is associated with individually named users.
17. (Original) The method of claim 13 in which the access control point is associated with a group of users.
18. (Original) The method of claim 17 in which members of the group are associated with a set of access privileges associated with the access control point.
19. (Currently Amended) A system for managing user access information for one or more database network nodes, comprising:
 - a LDAP directory;
 - one or more database network nodes for which user access is sought, wherein the one or more database network nodes are associated with the LDAP directory; and
 - user access information data objects stored in the LDAP directory, the user access information data objects comprising authentication and authorization information, wherein the authorization information is associated with a scope of access for a user;
 - wherein the user access information data objects are associated with an enterprise role, the enterprise role comprising a collection of roles, one of the collection of roles associated with a privilege that is locally defined at one of the one or more database network nodes associated with one or more databases, one of the data objects comprising a distinguished name that does not include a user name.
20. (Original) The system of claim 19 in which the user access information data objects comprise a domain object that is associated with the one or more database network nodes.

21. (Previously Presented) The system of claim 20 in which the domain object is associated with the enterprise role.
22. (Original) The system of claim 21 in which the enterprise role is associated with a local database role.
23. (Original) The system of claim 22 in which the scope of the local database role is locally defined at a local database network node.
24. (Currently Amended) The system of claim 21 in which the enterprise role is associated with ~~one more users~~ another user.
25. (Canceled).
26. (Original) The system of claim 19 in which the user access information data objects comprise an access control point attribute.
27. (Original) The system of claim 26 in which the access control point attribute is established only if access control policies are established for a corresponding object.
28. (Original) The system of claim 26 in which the access control point attribute is associated with access policies for a subtree in the user access information data objects stored in the LDAP directory.
29. (Original) The system of claim 26 in which the access control point attribute is associated with access policies for a single entry in the user access information data objects stored in the LDAP directory.
30. (Original) The system of claim 26 in which the access control point attribute is associated with individually named users.

31. (Original) The system of claim 26 in which the access control point attribute is associated with a group of users.
32. (Previously Presented) The system of claim 31 in which members of the group are associated with a set of access privileges associated with the access control.
33. (Original) The system of claim 19 in which the user access information data objects comprise a mapping object that maps an database user to a database schema.
34. (Original) The system of claim 33 in which the mapping object affects a single user.
35. (Original) The system of claim 34 in which the mapping object is associated with a full distinguished name.
36. (Original) The system of claim 33 in which the mapping object is associated with a plurality of users.
37. (Original) The system of claim 36 in which the mapping object is associated with a partial distinguished name.
38. (Original) The system of claim 21 in which the enterprise role is associated with local database roles from a plurality of database nodes.
39. (Currently Amended) A computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process for managing user access information for database network nodes, the process comprising:

storing database user authorization in a central directory that is ~~connected~~ associated with
~~to one or more databases~~ network nodes, the database user authorization comprising a user role,
~~the user role comprising one or more privileges;~~

storing database user authentication information;

locally ~~defining~~ associating the user role that is at the central directory with one or more
privileges, wherein the act of locally associating is performed at a one of the network node nodes
that is associated with the central directory;

receiving an access request from a user for the network node;

authenticating the user based upon the database user authentication information; and

granting the user privileges on the network node based upon the user role;

wherein the database user authorization is stored as one or more data-objects in the
central directory, ~~and one of the one or more data-objects comprises a distinguished name that~~
~~does not include a user name.~~

40. (Previously Presented) The computer program product of claim 39 in which the central
directory comprises a LDAP-compatible directory.

41. (Previously Presented) The computer program product of claim 39 in which the database
user authentication information is stored at the central directory.

42. (Previously Presented) The computer program product of claim 39 in which the database
user authorization is stored in a schema having a hierarchy of schema objects.

43. (Canceled)

44. (Previously Presented) The computer program product of claim 39 in which the one or
more objects are stored in a security subtree in the central directory.

45. (Previously Presented) The computer program product of claim 39 in which
administrative access is controlled to one or more data objects in the central directory.

46. (Previously Presented) The computer program product of claim 45 in which access control is implemented using an access control point associated with the one or more data objects in the central directory.
47. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory.
48. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory.
49. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with individually named users.
50. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with a group of users.
51. (Previously Presented) The computer program product of claim 50 in which members of the group are associated with a set of access privileges associated with the access control point.
52. (New) The method of claim 1, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for identifying a database.
53. (New) The method of claim 1, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for representing an administrative context, a root context, or a user-fined context.

54. (New) The method of claim 1, wherein the one or more privileges are locally defined at the one of the network nodes.
55. (New) The method of claim 54, wherein the database user authorization is stored in the central directory such that central management of the user role may be performed.
56. (New) The method of claim 54, wherein the one or more privileges are not centrally defined at the central directory.